VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
PHD 99.099WO			
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*		(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 99/07012	17/09/1999		30/09/1998
Anmelder			
KONINKLIJKE PHILIPS ELECTRONICS N.V. et al.			

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 2

   [X] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

THIS PAGE BLANK

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
[redacted]/EP 99/07012

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L H04K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
E	FR 2 776 445 A (SCHLUMBERGER IND SA) 24. September 1999 (1999-09-24) Spalte 1, Zeile 12 - Zeile 18 Spalte 2, Zeile 23 - Zeile 32 Spalte 3, Zeile 25 - Zeile 32 Spalte 4, Zeile 8 - Zeile 14 ---	1-3,6-8, 12,14
X	ADLER: "Cryptographic Device. March 1974." IBM TECHNICAL DISCLOSURE BULLETIN, Bd. 16, Nr. 10, Seiten 3406-3409, XP002128176 New York, US Seite 3407, Zeile 1 - Zeile 28 --- -/--	1,2,8

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
19. Januar 2000	02/02/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

Internationales Aktenzeichen
PCT/EP 99/07012

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 4 176 247 A (ENGLUND ROBERT M) 27. November 1979 (1979-11-27) Zusammenfassung Spalte 1, Zeile 12 - Zeile 16 Spalte 1, Zeile 41 - Zeile 51 Spalte 4, Zeile 23 - Zeile 41; Abbildung 2 ---	1,8
A	US 5 091 941 A (NEEDLE DAVID L ET AL) 25. Februar 1992 (1992-02-25) Zusammenfassung; Abbildung 3 -----	1,6,8

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/EP 99/07012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2776445 A	24-09-1999	AU 2842299 A	11-10-1999
		WO 9948239 A	23-09-1999
US 4176247 A	27-11-1979	NONE	
US 5091941 A	25-02-1992	DE 4135061 A	07-05-1992
		GB 2250163 A	27-05-1992
		JP 6029968 A	04-02-1994

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H04L 9/06

A1

(11) Internationale Veröffentlichungsnummer: WO 00/19656

(43) Internationales Veröffentlichungsdatum: 6. April 2000 (06.04.00)

(21) Internationales Aktenzeichen: PCT/EP99/07012

(22) Internationales Anmeldedatum: 17. September 1999 (17.09.99)

(30) Prioritätsdaten:

198 45 095.8	30. September 1998 (30.09.98)	DE
199 36 918.6	5. August 1999 (05.08.99)	DE

(81) Bestimmungsstaaten: JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht

Mit internationalem Recherchenbericht.

Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL–5621 BA Eindhoven (NL).

(71) Anmelder *(nur für DE)*: PHILIPS CORPORATE INTELLECTUAL PROPERTY GMBH [DE/DE]; Habsburgerallee 11, D–52066 Aachen (DE).

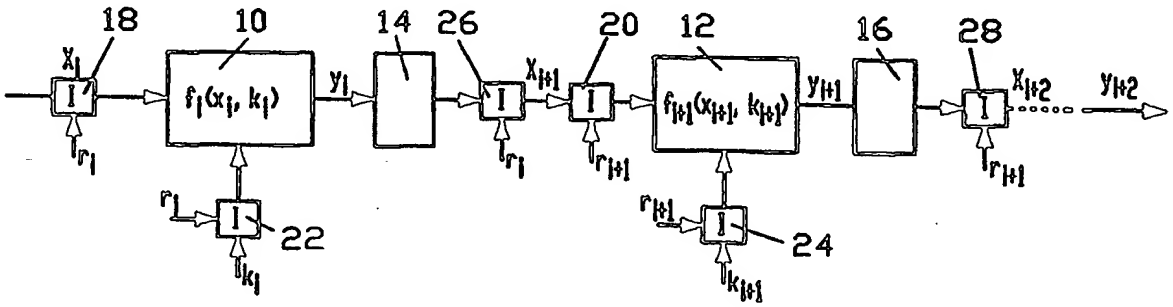
(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: PHILIPP, Stefan [DE/NL]; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(74) Anwalt: PETERS, Carl, H.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(54) Title: ENCODING METHOD FOR CARRYING OUT CRYPTOGRAPHIC OPERATIONS

(54) Bezeichnung: VERSCHLÜSSELUNGSVERFAHREN ZUM AUSFÜHREN VON KRYPTOGRAPHISCHEN OPERATIONEN



(57) Abstract

The invention relates to an encoding method and an encoding device. At least one partial cryptographic operation $y_i=f_i(x_i, k_i)$ is carried out by data x_i, k_i which are digitally stored as data bit words and the result or intermediate results y_i are digitally stored or temporarily stored as data bit words. At least one of the data x_i, k_i and/or the result or at least intermediate result y_i is optionally complemented or not bit by bit to $\overline{x}_i$, $\overline{k}_i$ and/or $\overline{y}_i$, in accordance with a control signal r_i based on random numbers.

(57) Zusammenfassung

Die vorliegende Erfindung betrifft ein Verschlüsselungsverfahren sowie eine Verschlüsselungsvorrichtung, wobei wenigstens eine kryptographische Teiloperation $y_i=f_i(x_i, k_i)$ von digital als Datenbitworte gespeicherten Daten x_i, k_i ausgeführt und das jeweilige Ergebnis bzw. jeweilige Zwischenergebnisse y_i digital als Datenbitworte abgespeichert bzw. zwischengespeichert werden. Hierbei wird wenigstens eines der Daten x_i, k_i und/oder das Ergebnis bzw. wenigstens ein Zwischenergebnis y_i in Abhängigkeit von einem auf Zufallszahlen basierenden Steuersignal r_i wahlweise bitweise zu $\overline{x}_i$, $\overline{k}_i$ und/oder $\overline{y}_i$ komplementiert oder nicht.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verschlüsselungsverfahren zum Ausführen von kryptographischen Operationen.

Die Erfindung betrifft ein Verschlüsselungsverfahren, wobei wenigstens eine kryptographische Teiloperation $y_i=f_i(x_i, k_i)$ von digital als Datenbitworte gespeicherten Daten x_i, k_i ausgeführt und das jeweilige Ergebnis bzw. jeweilige Zwischenergebnisse y_i digital als Datenbitworte abgespeichert bzw. zwischengespeichert werden, gemäß dem Oberbegriff des Anspruchs 1. Die Erfindung betrifft ferner eine Verschlüsselungsvorrichtung mit einer Berechnungseinheit und Registern R_i, wobei die Berechnungseinheit wenigstens eine kryptographische Teiloperation $y_i=f_i(x_i, k_i)$ von digital in den Registern R_i der Verschlüsselungsvorrichtung als Datenbitworte gespeicherten Operanden x_i, k_i ausführt und das jeweilige Ergebnis bzw. Zwischenergebnisse y_i digital in den Registern R_i der Verschlüsselungsvorrichtung als Datenbitworte abspeichert bzw. zwischenspeichert, gemäß dem Oberbegriff des Anspruchs 8.

In vielen Datenverarbeitungsgeräten dienen kryptographische Operationen zum Schutz des Betriebes dieser Geräte bzw. zum Schutz von in dem Gerät transportierten Daten. Die hierfür notwendigen Berechnungsoperationen werden dabei sowohl von Standard-Rechenwerken als auch von dedizierten Crypto-Rechenwerken durchgeführt. Ein typisches Beispiel für letzteres sind Chipkarten bzw. IC-Karten. Bei derartigen kryptographischen Berechnungen, wie in Fig. 1 veranschaulicht, ist es oftmals notwendig, entsprechende Speicherbereiche bzw. Register des Datenverarbeitungsgerätes mit Operanden x_i, k_i zu initialisieren. Während der i-ten Berechnung werden ggf. Zwischenergebnisse y_i in Speicherbereichen oder Registern R_i abgelegt oder abschließend das Ergebnis der Berechnung zur Weiterverarbeitung in Speicherbereichen oder Registern abgelegt. Das Register r_i befindet sich zwischen einer vorherigen i-ten kryptographischen Berechnung und einer nachfolgenden (i+1)-ten kryptographischen Berechnung. Bei den in diesem Zusammenhang verwendeten Daten x_i, k_i bzw. Zwischenergebnissen y_i handelt es sich üblicherweise um sicherheitsrelevante Informationen, wie beispielsweise kryptographische Schlüssel oder Operanden.

Zur Berechnung der kryptographischen Algorithmen werden in den Datenverarbeitungsgeräten logische Verknüpfungen zwischen Operanden k_i bzw. Zwischenergebnissen y_i bzw. x_i, x_{i+1} durchgeführt. In Abhängigkeit von der verwendeten Technologie führen diese Operationen, insbesondere das Laden der Speicherbereiche bzw. Register mit Daten, zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei komplementärer Logik, wie beispielsweise der CMOS-Technik, tritt ein erhöhter Stromverbrauch dann auf, wenn der Wert einer Bit-Speicherzelle geändert wird, d.h. sein Wert sich von "0" auf "1" bzw. von "1" auf "0" ändert. Der erhöhte Verbrauch hängt dabei von der Anzahl der im Speicher bzw. Register geänderten Bitstellen ab. Mit anderen Worten lässt das Laden eines zuvor gelöschten Registers einen Stromverbrauch proportional zum Hamminggewicht des Operanden (=Anzahl der Bits mit dem Wert "1") bzw. der Differenz im Hamminggewicht ansteigen. Durch eine entsprechende Analyse dieser Stromänderung könnte es möglich sein, Informationen über die berechneten Operationen zu extrahieren, so dass eine erfolgreiche Kryptoanalyse von geheimen Operanden, wie beispielsweise kryptographischen Schlüsseln, möglich ist. Mittels Durchführung mehrerer Strommessungen am Datenverarbeitungsgerät könnten beispielsweise bei sehr kleinen Signaländerungen eine hinreichende Extraktion der Informationen ermöglicht werden. Andererseits könnten mehrere Strommessungen eine ggf. erforderliche Differenzbildung ermöglichen. Diese Art der Kryptoanalyse wird auch als "Differential Power Analysis" bezeichnet, mittels derer ein Außenstehender durch reine Beobachtung von Änderungen des Stromverbrauches des Datenverarbeitungsgerätes eine ggf. unberechtigte Kryptoanalyse der kryptographischen Operationen, Algorithmen, Operanden bzw. Daten erfolgreich ausführen kann.

Aus der US 5 297 201 ist es bekannt, einen Hochfrequenz abstrahlenden Computer mit einer Einrichtung zu kombinieren, welche ebenfalls Hochfrequenz ähnlich zu derjenigen des Computers abstrahlt. Dadurch ist es für einen unberechtigten Dritten nicht mehr möglich, die Hochfrequenzabstrahlung des Computers zu dekodieren. Eine Kryptoanalyse durch einen Dritten, der unmittelbar Zugang zum Computer hat, kann dieses System jedoch nicht verhindern.

Um bei Chipkarten eine Korrelation zwischen einer Ausgabe eines Ergebnisses einer kryptographischen Operation bzw. einer Übertragung einer Schlüsselinformation für eine kryptographischen Operation und der kryptographischen Operation selbst zu beseitigen ist es aus Patent Abstracts of Japan 10069222A bekannt, das Ergebnis der kryptographischen Operation bzw. die Übertragung der Schlüsselinformation für die kryptographischen

Operationen zeitlich zu verzögern. Jedoch ist auch dieses System mittels der "Differential Power Analysis" analysierbar, da sich auch die verzögerte Datenübertragung im Stromverbrauch des Datenverarbeitungsgerätes verrät.

Es ist Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren sowie eine verbesserte Vorrichtung der obengenannten Art zur Verfügung zu stellen, welche die obengenannten Nachteile beseitigen und eine erfolgreiche Kryptoanalyse mittels Beobachtung eines Stromverbrauches eines Datenverarbeitungsgerätes wirksam verhindert.

Diese Aufgabe wird durch ein Verfahren der o.g. Art mit den in Anspruch 1 gekennzeichneten Merkmalen gelöst.

Dazu ist es erfindungsgemäß vorgesehen, dass wenigstens eines der Daten x_i, k_i und/oder das Ergebnis bzw. wenigstens ein Zwischenergebnis y_i in Abhängigkeit von einem auf Zufallszahlen basierenden Steuersignal r_i wahlweise bitweise zu $\bar{y}=f(\bar{x},\bar{k})$ und/oder $\bar{y}_i$ komplementiert wird oder nicht.

Dies hat den Vorteil, dass bei wiederholter Ausführung derselben kryptographischen Operation andere Bitfolgen bearbeitet bzw. abgespeichert werden, so dass sich bei der jeweiligen Ausführung einer kryptographischen Operation bzw. mehrerer kryptographischer Operationen andere Stromänderungen des Datenverarbeitungsgerätes ergeben. Unabhängig vom eigentlichen Wert der Teilergebnisse wird somit bei wiederholter Ausführung der Gesamtberechnung erreicht, dass jeder Datenpfad bei einer echten Zufallszahlenreihe gleichhäufig bzw. bei einer Pseudozufallszahlenreihe nahezu gleichhäufig von "0" auf "0", von "0" auf "1", von "1" auf "0" und von "1" auf "1" wechselt. Da jedoch das auf Zufallszahlen basierende Steuersignal r_i nicht bekannt bzw. vorbestimmt ist, fehlt eine Korrelation zwischen den Stromänderungen und den Bitwerten der Daten und Ergebnisse, so dass eine "Differential Power Analysis" nicht mehr zu einer erfolgreichen Kryptoanalyse führt. Mit anderen Worten enthält der mittlere Stromverbrauch der Gesamtoperation keine brauchbare Information über die verwendeten Teiloperanden bzw. Zwischenergebnisse in den Teiloperationen.

Vorzugsweise Weitergestaltungen der Vorrichtung sind in den Ansprüchen 2 bis 7 beschrieben.

Zweckmäßigerweise werden in den kryptographischen Teiloperationen eine oder mehrere XOR-Verknüfungen (Exklusiv-Oder-Verknüfung) ausgeführt.

Die Daten umfassen beispielsweise kryptographische Schlüssel und/oder Operanden.

In einer bevorzugten Ausführungsform werden Zwischenergebnisse y_i zwischen der Ausführung von aufeinander folgenden kryptographischen Teiloperationen in einem Register R_i zwischengespeichert und als Operand x_{i+1} der nachfolgenden kryptographischen Teiloperationen zugeführt.

Zum Herstellen eines originalen, nicht invertierten Wertes nach jeder Teiloperation wird eine aus dem Zwischenergebnis y_i einer vorangegangenen Teiloperation i erhaltene Bitfolge $x_{i+1} = y_i$ für eine nachfolgende Teiloperation i+1 bitweise zu $\overline{x}_{i+1}$ komplementiert, wenn die Daten x_i, k_i der vorangegangenen Teiloperation i bitweise komplementiert wurden.

In einer besonders bevorzugten Ausführungsform werden bei der bitweisen Komplementierung wenigstens ein Bitwert, insbesondere die geraden Bitwerte, die ungeraden Bitwerte oder alle Bitwerte, eines Datenbitwortes x_i, k_i, bzw. y_i invertiert. Hierbei ist es besonders vorteilhaft, wenn eine Invertierung von Bitwerten bzw. Bitadressen eines Datenbitwortes x_i, k_i, bzw. y_i bei der bitweisen Komplementierung mittels einer XOR-Operation (Exklusiv-Oder-Operation) durchgeführt wird.

Bei einer Vorrichtung der o.g. Art ist erfindungsgemäß wenigstens ein von einem Steuersignal r_i steuerbarer Inverter für wenigstens eines der Daten x_i, k_i und/oder das Ergebnis bzw. wenigstens ein Zwischenergebnis y_i, ein Zufallszahlengenerator, welcher Zufallszahlen erzeugt, sowie eine Vorrichtung zum Erzeugen des Steuersignals r_i auf den Zufallszahlen basierend vorgesehen, wobei der steuerbare Inverter in Abhängigkeit von dem Steuersignal r_i wahlweise die Bitfolgen x_i, k_i bzw. y_i zu ihrem bitweisen Komplement $\overline{x}_i$, $\overline{k}_i$ bzw. $\overline{y}_i$ umsetzt oder unverändert lässt.

Dies hat den Vorteil, dass bei wiederholter Ausführung derselben kryptographischen Operation andere Bitfolgen bearbeitet bzw. abgespeichert werden, so dass sich bei der jeweiligen Ausführung der kryptographischen Operation bzw. kryptographischen Operationen andere Stromänderungen des Datenverarbeitungsgerätes ergeben. Unabhängig vom eigentlichen Wert der Teilergebnisse wird somit bei wiederholter Ausführung der Gesamtberechnung erreicht, dass jeder Datenpfad bei einer echten Zufallszahlenreihe gleichhäufig bzw. bei einer Pseudozufallszahlenreihe nahezu gleichhäufig von "0" auf "0", von "0" auf "1", von "1" auf "0" und von "1" auf "1" wechselt. Da jedoch das auf Zufallszahlen basierende Steuersignal r_i nicht bekannt bzw. vorbestimmt ist, fehlt eine Korrelation zwischen

den Stromänderungen und den Bitwerten der Daten und Ergebnisse, so dass eine "Differential Power Analysis" nicht mehr zu einer erfolgreichen Kryptoanalyse führt. Mit anderen Worten enthält der mittlere Stromverbrauch der Gesamtoperation keine brauchbare Information über die verwendeten Teiloperanden bzw. Zwischenergebnisse in den Teiloperationen.

Vorzugsweise Weitergestaltungen der Vorrichtung sind in den Ansprüchen 9 bis 14 beschrieben.

In einer bevorzugten Ausführungsform ist wenigstens einem Register R_i ein Inverter nachgeschaltet, welcher das identische Steuersignal r_i erhält, wie die der i-ten Teiloperation vorgeschalteten Inverter für die Daten x_i, k_i. Dieser einem Register R_i der i-ten Teiloperation nachgeschaltete Inverter ist dabei bevorzugt mit einem der nachfolgenden (i+1)-ten Teiloperation vorgeschalteten Inverter für ein Eingangsdatum x_{i+1} kombiniert. Der kombinierte Inverter erhält zweckmäßigerweise sowohl das Steuersignal r_i der vorangegangenen i-ten Teiloperation als auch das Steuersignal r_{i+1} der nachfolgenden (i+1)-ten Teiloperation.

Die Daten umfassen beispielsweise kryptographische Schlüssel und/oder Operanden.

In einer bevorzugten Ausführungsform speichert ein Register R_i zwischen einer vorangegangenen i-ten Teiloperation und einer nachfolgenden (i+1)-ten Teiloperation ein Zwischenergebnis y_i der vorangegangenen i-ten Teiloperation und leitet dieses Zwischenergebnis als Eingangswert x_{i+1} an die nachfolgende (i+1)-te Teiloperation weiter.

Zweckmäßigerweise invertiert die bitweise Komplementierung wenigstens einen Bitwert, insbesondere die geraden Bitwerte, die ungeraden Bitwerte oder alle Bitwerte, eines Datenbitwortes x_i, k_i, bzw. y_i.

Nachstehend wird die Erfindung anhand der beigefügten Zeichnungen näher erläutert. Diese zeigen in

Fig. 1 ein Ablaufschema eines Teiles einer kryptographischen Operation gemäß dem Stand der Technik,

Fig. 2 ein Ablaufschema eines Teiles einer ersten bevorzugten Ausführungsform einer erfindungsgemäßen kryptographischen Operation und

Fig. 3 ein Ablaufschema eines Teiles einer zweiten bevorzugten Ausführungsform einer erfindungsgemäßen kryptographischen Operation.

Bei der in Fig. 2 dargestellten ersten bevorzugten Ausführungsform eines erfindungsgemäßen Verschlüsselungsverfahrens wird durch eine Kette von Teiloperationen $f_i(x_i, k_i)$, innerhalb derer ein oder mehrere logische XOR-Verknüpfungen (Exklusiv-Oder-Verknüpfung) ausgeführt werden, eine kryptographische Gesamtoperation durchgeführt. Dargestellt sind zwei Teiloperationen, nämlich die i-te Teiloperation 10 und die (i+1)-te Teiloperation 12, wobei jede Teiloperation von einer Berechnungseinheit ausgeführt wird. Jeder Teiloperation 10, 12 ist eine Speicherzelle oder ein Register R_i 14 bzw. eine Speicherzelle oder ein Register R_i 16 nachgeschaltet. Jede Teiloperation 10, 12 hat als Eingangswert ein Datum x_i, x_{i+1} sowie einen Operanden k_i, k_{i+1}, welche als Datenbitworte zur Verfügung stehen.

Jeder Teiloperation 10, 12 vorgeschaltet ist jeweils ein steuerbarer Inverter 18 bzw. 20 für die Daten x_i, x_{i+1} sowie jeweils ein steuerbarer Inverter 22, 24 für die Operanden k_i, k_{i+1}. Ferner ist bei jeder Teiloperation 10, 12 dem jeweiligen Register R_i 14 bzw. R_{i+1} 16 ein steuerbarer Inverter 26, 28 für das Zwischenergebnis y_i, y_{i+1} nachgeschaltet, wobei dieses Zwischenergebnis von dem jeweiligen Register R_i 14 bzw. R_{i+1} 16 als Eingangsdaten x_{i+1} bzw. x_{i+2} an eine nachfolgende Teiloperation 12 weiter gegeben werden. Diese Inverter 18 bis 28 sind durch ein Steuersignal r_i bzw. r_{i+1} derart steuerbar, dass sie in Abhängigkeit von dem jeweiligen Steuersignal r_i bzw. r_{i+1} wahlweise die zugeordneten Datenbitworte bitweise komplementieren oder nicht. Hierbei erhalten alle Inverter 18, 22, 26 bzw. 20, 24, 28 einer Teiloperation 10 bzw. 12 dasselbe Steuersignal r_i bzw. r_{i+1}. Mit anderen Worten wird die Entscheidung, ob eine Invertierung der entsprechenden Eingangswerte der Inverter 18 bis 28 durchgeführt wird oder ob die Eingangswerte unbearbeitet die Inverter 18 bis 28 durchlaufen, durch das zusätzliche Steuersignal r_i bzw. r_{i+1} entschieden. Diese Anordnung von Registern 14, 16 zwischen Teiloperationen 10, 12 findet vor allem dann Anwendung, wenn die Teiloperationen 10, 12 zeitlich nacheinander von ein und derselben Einheit berechnet werden und somit die Teilergebnisse zwischengespeichert werden müssen.

Das Steuersignal wird durch Zufallswerte aus einem Zufallsgenerator dahingehend gesteuert, dass die Teiloperation abhängig vom Wert der Zufallszahlen entweder das Originalergebnis $y = f(x, k)$ oder das bitinvertierte Ergebnis $\bar{y} = f(\bar{x}, \bar{k})$ liefert. Hierdurch wird realisiert, dass sowohl die Berechnung als auch die Speicherung der Daten in den Registern R_i 14, 18 entweder mit Originalwerten oder mit bitinvertierten Werten durchgeführt wird. Unabhängig vom eigentlichen Wert der Teilergebnisse wird somit bei wiederholter Ausführung der Gesamtberechnung erreicht, dass jeder Datenpfad gleich häufig von "0" auf

"0", von "0" auf "1", von "1" auf "0" und von "1" auf "1" wechselt. Der mittlere Stromverbrauch der Gesamtoperation enthält somit keine brauchbare Information über die verwendeten Teiloperanden k_i bzw. Zwischenergebnisse y_i in den Teiloperationen 10, 12. Der dem Register 14, 16 nachgeschaltete Inverter 26, 28 stellt für die folgende Teiloperation 12 wieder den originalen, nicht invertierten Wert her.

Die zweite bevorzugte Ausführungsform des erfindungsgemäßen Verschlüsselungsverfahrens gemäß Fig. 3 entspricht der ersten Ausführungsform von Fig. 2 mit dem einzigen Unterschied, dass die den Registern 14, 16 nachgeschalteten Inverter 26, 28 mit dem jeweiligen Eingangsinverter 20 der folgenden Stufe 12 zu einem Inverter 30 kombiniert sind.

Die Inverter invertieren beispielsweise auch nur einen Teil der Bitwerte des jeweiligen Datenbitwortes. So werden beispielsweise nur die geraden oder ungeraden Bitworte bzw. Bitadressen invertiert. Die Invertierung der Bitwerte erfolgt beispielsweise mittels einer XOR-Operation (Exklusiv-Oder-Operation).

BEZUGSZEICHENLISTE:

10	i-te Teiloperation
12	(i+1)-te Teiloperation
14	Register R_i
16	Register R_{i+1}
18	steuerbarer Inverter für x_i
20	steuerbarer Inverter für x_{i+1}
22	steuerbarer Inverter für k_i
24	steuerbarer Inverter für k_{i+1}
26	steuerbarer Inverter für y_i
28	steuerbarer Inverter für y_{i+1}
30	kombinierter Inverter

PATENTANSPRÜCHE:

1. Verschlüsselungsverfahren, wobei wenigstens eine kryptographische Teiloperation $y_i=f_i(x_i, k_i)$ von digital als Datenbitworte gespeicherten Daten x_i, k_i ausgeführt und das jeweilige Ergebnis bzw. jeweilige Zwischenergebnisse y_i digital als Datenbitworte abgespeichert bzw. zwischengespeichert werden,
dadurch gekennzeichnet, dass
wenigstens eines der Daten x_i, k_i und/oder das Ergebnis bzw. wenigstens ein Zwischenergebnis y_i in Abhängigkeit von einem auf Zufallszahlen basierenden Steuersignal r_i wahlweise bitweise zu $\overline{x}_i$, $\overline{k}_i$ und/oder $\overline{y}_i$ komplementiert wird oder nicht.

2. Verschlüsselungsverfahren nach Anspruch 1,
dadurch gekennzeichnet, dass
in den kryptographischen Teiloperationen eine oder mehrere XOR-Verknüpfungen (Exklusiv-Oder-Verknüpfung) ausgeführt werden.

3. Verschlüsselungsverfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet, dass
die Daten kryptographische Schlüssel und/oder Operanden umfassen.

4. Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass
Zwischenergebnisse y_i zwischen der Ausführung von aufeinander folgenden kryptographischen Teiloperationen in einem Register R_i zwischengespeichert und als Operand x_{i+1} der nachfolgenden kryptographischen Teiloperationen zugeführt werden.

5. Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass
eine aus dem Zwischenergebnis y_i einer vorangegangenen Teiloperation i erhaltene Bitfolge $x_{i+1} = y_i$ für eine nachfolgende Teiloperation i+1 bitweise zu $\overline{x}_{i+1}$ komplementiert wird, wenn die Daten x_i, k_i der vorangegangenen Teiloperation i bitweise komplementiert wurden.

6. Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass
bei der bitweisen Komplementierung wenigstens ein Bitwert, insbesondere die geraden Bitwerte, die ungeraden Bitwerte oder alle Bitwerte, eines Datenbitwortes x_i, k_i, bzw. y_i invertiert werden.

7. Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass
eine Invertierung von Bitwerten bzw. Bitadressen eines Datenbitwortes x_i, k_i, bzw. y_i bei der bitweisen Komplementierung mittels einer XOR-Operation (Exklusiv-Oder-Operation) durchgeführt wird.

8. Verschlüsselungsvorrichtung mit einer Berechnungseinheit und Registern R_i (14, 16), wobei die Berechnungseinheit wenigstens eine kryptographische Teiloperation $y_i=f_i(x_i, k_i)$ (10, 12) von digital in den Registern R_i (14, 16) der Verschlüsselungsvorrichtung als Datenbitworte gespeicherten Operanden x_i, k_i ausführt und das jeweilige Ergebnis bzw. Zwischenergebnisse y_i digital in den Registern R_i (14, 16) der Verschlüsselungsvorrichtung als Datenbitworte abspeichert bzw. zwischenspeichert,
dadurch gekennzeichnet, dass
wenigstens ein von einem Steuersignal r_i steuerbarer Inverter (18 bis 28; 30) für wenigstens eines der Daten x_i, k_i und/oder das Ergebnis bzw. wenigstens ein Zwischenergebnis y_i, ein Zufallszahlengenerator, welcher Zufallszahlen erzeugt, sowie eine Vorrichtung zum Erzeugen des Steuersignal r_i auf den Zufallszahlen basierend vorgesehen ist, wobei der steuerbare Inverter (18 bis 28; 30) in Abhängigkeit von dem Steuersignals r_i wahlweise die Bitfolgen x_i, k_i bzw. y_i zu ihrem bitweisen Komplement $\overline{x}_i$, $\overline{k}_i$ bzw. $\overline{y}_i$ umsetzt oder unverändert lässt.

9. Verschlüsselungsvorrichtung nach Anspruch 8,
dadurch gekennzeichnet, dass
wenigstens einem Register R_i (14, 16) ein Inverter (26, 28; 30) nachgeschaltet ist, welcher das identische Steuersignal r_i erhält, wie die der i-ten Teiloperation (10, 12) vorgeschalteten Inverter (18, 20) für die Daten x_i, k_i.

10. Verschlüsselungsvorrichtung nach Anspruch 9,

dadurch gekennzeichnet, dass
der einem Register R_i (14, 16) der i-ten Teiloperation (10, 12) nachgeschaltete Inverter (26, 28) mit einem der nachfolgenden (i+1)-ten Teiloperation (12) vorgeschalteten Inverter (20) für ein Eingangsdatum x_{i+1} kombiniert ist.

11. Verschlüsselungsvorrichtung nach Anspruch 10,
dadurch gekennzeichnet, dass
der kombinierte Inverter (30) sowohl das Steuersignal r_i der vorangegangenen i-ten Teiloperation (10) als auch das Steuersignal r_{i+1} der nachfolgenden (i+1)-ten Teiloperation (12) erhält.

12. Verschlüsselungsvorrichtung nach einem der Ansprüche 8 bis 11,
dadurch gekennzeichnet, dass
die Daten kryptographische Schlüssel und/oder Operanden umfassen.

13. Verschlüsselungsvorrichtung nach einem der Ansprüche 8 bis 12,
dadurch gekennzeichnet, dass
ein Register R_i (14, 16) zwischen einer vorangegangenen i-ten Teiloperation (10) und einer nachfolgenden (i+1)-ten Teiloperation (12) ein Zwischenergebnis y_i der vorangegangenen i-ten Teiloperation (10) speichert und dieses Zwischenergebnis als Eingangswert x_{i+1} an die nachfolgende (i+1)-te Teiloperation (12) weiterleitet.

14. Verschlüsselungsvorrichtung nach einem der Ansprüche 8 bis 13,
dadurch gekennzeichnet, dass
die bitweise Komplementierung wenigstens einen Bitwert, insbesondere die geraden Bitwerte, die ungeraden Bitwerte oder alle Bitwerte, eines Datenbitwortes x_i, k_i, bzw. y_i invertiert.

1/1

Fig.1

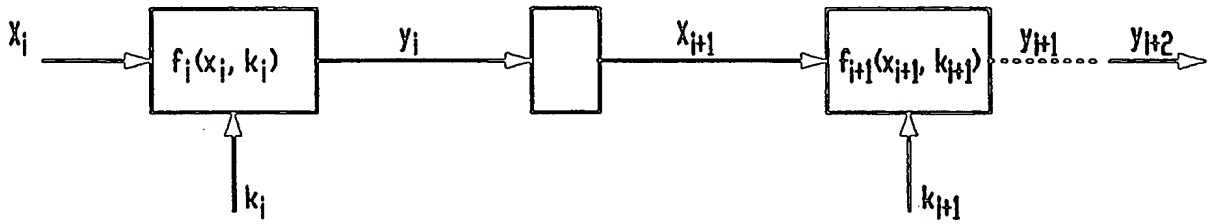


Fig.2

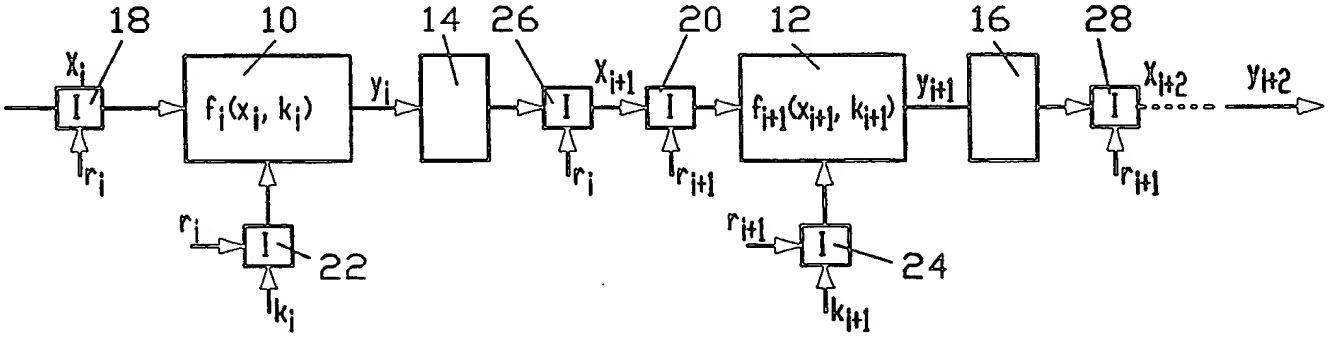
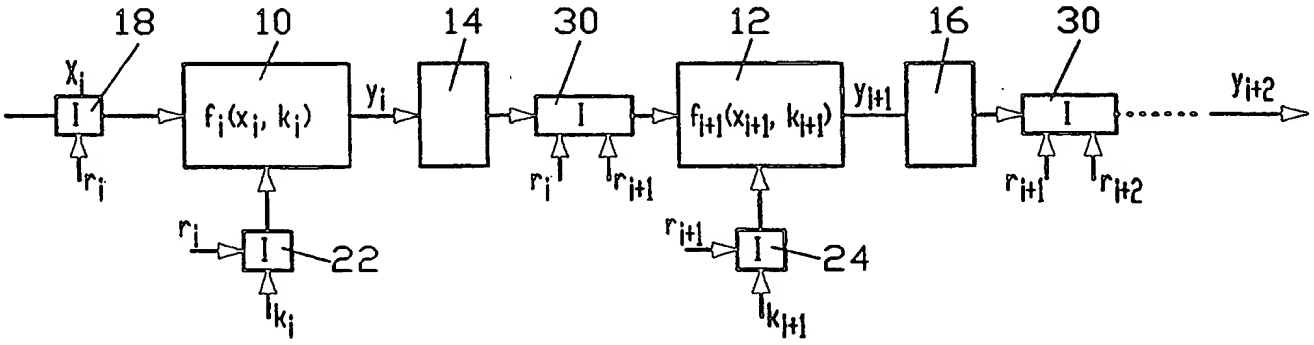


Fig.3



INTERNATIONAL SEARCH REPORT

Inte[illegible]ional Application No
PCT/EP 99/07012

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	FR 2 776 445 A (SCHLUMBERGER IND SA) 24 September 1999 (1999-09-24) column 1, line 12 - line 18 column 2, line 23 - line 32 column 3, line 25 - line 32 column 4, line 8 - line 14 ---	1-3,6-8, 12,14
X	ADLER: "Cryptographic Device. March 1974." IBM TECHNICAL DISCLOSURE BULLETIN, vol. 16, no. 10, pages 3406-3409, XP002128176 New York, US page 3407, line 1 - line 28 --- -/--	1,2,8

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 January 2000	02/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 176 247 A (ENGLUND ROBERT M) 27 November 1979 (1979-11-27) abstract column 1, line 12 - line 16 column 1, line 41 - line 51 column 4, line 23 - line 41; figure 2	1,8
A	US 5 091 941 A (NEEDLE DAVID L ET AL) 25 February 1992 (1992-02-25) abstract; figure 3	1,6,8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 99/07012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2776445 A	24-09-1999	AU 2842299 A	11-10-1999
		WO 9948239 A	23-09-1999
US 4176247 A	27-11-1979	NONE	
US 5091941 A	25-02-1992	DE 4135061 A	07-05-1992
		GB 2250163 A	27-05-1992
		JP 6029968 A	04-02-1994

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/07012

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L H04K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
E	FR 2 776 445 A (SCHLUMBERGER IND SA) 24. September 1999 (1999-09-24) Spalte 1, Zeile 12 - Zeile 18 Spalte 2, Zeile 23 - Zeile 32 Spalte 3, Zeile 25 - Zeile 32 Spalte 4, Zeile 8 - Zeile 14 ---	1-3,6-8, 12,14
X	ADLER: "Cryptographic Device. March 1974." IBM TECHNICAL DISCLOSURE BULLETIN, Bd. 16, Nr. 10, Seiten 3406-3409, XP002128176 New York, US Seite 3407, Zeile 1 - Zeile 28 --- -/--	1,2,8

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
19. Januar 2000	02/02/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)